IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 19, 2020, accepted November 4, 2020, date of publication November 10, 2020,
date of current version November 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3037180

Physical-Layer Security for Mobile Users in NOMA-Enabled Visible Light Communication Networks

XIANG ZHAO[1] AND JINYONG SUN[2]
[1]Key Laboratory of Cognitive Radio and Information Processing, Guilin University of Electronic Technology, Guilin 541004, China
[2]Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China

Corresponding author: Jinyong Sun (sunjy@guet.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61961007 and Grant 61862016, in part by the Guangxi Natural Science Foundation under Grant 2018GXNSFAA294093 and Grant 2017GXNSFAA198283, in part by the Guangxi Innovation Driven Development Special Fund under Grant AA18242030, in part by the Key Laboratory of Cognitive Radio and Information Processing (Guilin University of Electronic Technology) under Grant CRKL180108, in part by the Innovation Project of GUET Graduate Education under Grant 2020YCXS025, and in part by the Training Program Funding for Thousand Young and Middle-aged Backbone Teachers of Colleges and Universities in Guangxi.

ABSTRACT In view of the secrecy requirements of visible light communication (VLC) and the massive connectivity demand of future communication, this work investigates physical-layer security (PLS) for a VLC network based on nonorthogonal multiple access (NOMA). To date, however, research on PLS in NOMA-enabled VLC networks considers only users in a static state. The movements of users make it imperative to dynamically allocate optical access points (OAPs) and transmit power to mobile users (MUs). Such a resource allocation problem is transformed into the problem of dynamically allocating power in this paper. Thus, joint secure communication and power allocation optimization is formulated to maximize the network secrecy performance in each time frame subject to the constraint of the maximum power of OAPs and the constraint of power allocation based on NOMA among the associated MUs at each OAP. The formulated joint optimization problem is generally nonconvex because the logarithmic subtraction operation exists in the secrecy capacity, and we cannot directly find the optimal solution. A hierarchical power allocation algorithm is naturally proposed based on an iterative security-aware water-filling approach and the optimality conditions of Karush-Kuhn-Tucker. Convergence and effectiveness are investigated for the presented power allocation algorithms through simulations. The simulation results show that the network sum secrecy capacity depends on the number of MUs, the characteristics of the optical transceiver, and the number of OAPs deployed in the room.

INDEX TERMS Physical-layer security, visible light communication networks, PLS, mobile users, user mobility, nonorthogonal multiple access (NOMA).

I. INTRODUCTION

As the key technologies in fifth generation (5G) and beyond, visible light communication (VLC) and nonorthogonal multiple access (NOMA) have attracted widespread interest worldwide. On the one hand, VLC [1], [2] based on white light-emitting diodes (LEDs) can realize illumination and high-data rate communication with the existing lighting infrastructure to complement or be combined with current radio frequency (RF) communications networks, and it can be applied to many high user density scenarios, such as indoor shopping malls, exhibition or conference halls, and the waiting rooms of railway stations or airports, as well as outdoor intelligent transportation [3] and V2X communication, and thus VLC technology is suitable to support massive connectivity and high-speed low-latency communication which is exactly the requirement of future 5G and beyond [4]. On the other hand, NOMA [5], [6] makes it possible to serve multiple users with the same frequency or time resources and to separate them in the power domain or other domains, thus NOMA has an inherent nature of supporting massive connectivity. In addition, NOMA has the

The associate editor coordinating the review of this manuscript and approving it for publication was Tyson Brooks.

advantages of superior spectrum efficiency and low transmission latency compared with traditional orthogonal multiple access [7].

In recent years, as a promising alternative and complement to traditional encryption technology, physical-layer security (PLS) [8]–[10] has also gained much attention from academic and industry scientists. PLS technology utilizes the diversity and difference nature of wireless channels to mark each channel, including legitimate and eavesdropping channels, with a unique ''footprint''. PLS technology makes full use of the channel difference to distinguish users and to prevent legitimate users from being eavesdropped by eavesdropping users, directly ensuring secure transmission of information at the physical layer.

A. RELATED WORKS

Over the past five years, NOMA-enabled VLC networks have received extensive attention. NOMA is more suitable for VLC networks than for RF networks because 1) NOMA performs better in a high signal-to-noise ratio (SNR) environment [11], which is inherently offered in VLC systems because communication is performed on the basis of the infrastructure of LED illumination and, to achieve a certain dimming level, high transmission power is required. In addition, the indoor relatively short transmission distance and the dominant line of sight (LoS) path between LED transmitters and photodetector (PD) receivers can make the SNR high. 2) The broadcast nature of the wireless channel enables VLC to accommodate large numbers of users, while NOMA can efficiently multiplex multiple users. 3) The half-power angle of LED (i.e., the semiangle of an LED at half illuminance) and the field-of-view (FoV) of PD play an important part in improving VLC system performance. These two parameters can be used to tune the differences of the channel between users, which is critical for NOMA to achieve successive interference cancellation (SIC). *Much research on VLC networks based on NOMA has been undertaken.* To increase the achievable throughput for a NOMA-based VLC network, [11] presented a gain ratio power management approach. Considering the user fairness and optical intensity constraints, the sum throughput maximization problem was proposed in [12]. A detailed review of optical NOMA-VLC networks was conducted in [13], and to design and implement such a network, it also presented potential opportunities, challenges and open research problems. In a VLC network with multiple optical attocells, the time-sliced NOMA method was presented in [14] to cope with the interference between multiple users. For an unmanned aerial vehicle (UAV)-assisted VLC-NOMA network [15], NOMA power allocation and UAV location were jointly optimized to maximize the network throughput.

Over the past five years, research on PLS for VLC networks has also attracted great interest. Signal processing technologies such as beamforming [16], [17], precoding [18], [19], artificial optical jamming [20] and polar-code-based secure coding [21] are used to improve the secrecy performance of VLC. Taking the adopted mathematical tools into account, stochastic geometry theory was used to derive the average secrecy capacity of system while the users were randomly distributed in the room [22]. Optimization theory can also be used to enhance the secrecy performance of VLC systems while satisfying various constraints, such as the LED optical power constraint [23], the peak power constraint to reduce eye damage [16] and the light energy harvesting and dimming control constraint [17]. Taking the eavesdroppers into account, most researches on PLS for VLC networks were performed against external malicious eavesdroppers [16]–[18], [22], [23], while several have focused on the transmission of confidential information, that is to say, users are kept ignorant about the information not intended for them [19]. Note that only passive eavesdroppers were considered in the above mentioned papers. Recently, active and malicious attacks on VLC systems by malicious external nodes have begun to attract researchers' attention [24].

Since Zhang *et al.* [25] first studied PLS in NOMA networks in 2016, most work published on PLS in NOMA networks has focused on NOMA users eavesdropped or intercepted by external malicious eavesdroppers [25], [26]. Some users as untrusted nodes in relation to other legitimate NOMA users have also been investigated [27]. Both external and internal eavesdropping were considered in [28] to design secure transmission. In view of the adopted mathematical tools, optimization theory [25], stochastic geometry theory [26] and game theory [29] can be used to analyze the secrecy performance of NOMA systems. In view of the utilized signal processing technology, in addition to the above mentioned technology of PLS for VLC networks, transmit antenna selection [30] can also be utilized in PLS for NOMA systems. Not like PLS in VLC systems only focusing on downlink wireless communication, PLS in NOMA systems can also be applicable to uplink communication [31]. Moreover, PLS in NOMA applied to various systems such as mobile edge computing networks [31], UAV-assisted communication [32], [33], and ultra-dense networks [34] has gained much interest from researchers. However, these works on PLS in NOMA systems are all confined to the RF communication field and cannot be directly applied to the VLC field due to the particular characteristics of the optical transceiver and the optical wireless transmission channel.

To date, several studies on PLS in NOMA-enabled VLC networks have been conducted. For a multiuser, multi-external-eavesdropper downlink NOMA-VLC network, the secrecy outage probability (SOP) was derived in [35] based on the spatial distribution of users and eavesdroppers and the statistical characteristics of the optical wireless channel, and it illustrated that SOP performance is related to the parameters of the optical transceiver and the eavesdropping density. For a two-user single-external-eavesdropper downlink NOMA-VLC network, multiple trusted relays with the optical transceiver were deployed and secure beamforming vectors were designed in [36] to ensure secure transmission, showing that the best relaying scheme depends

on the geometric layout and the number of relays. To date, however, for research on PLS in NOMA-enabled VLC networks, only legitimate users in a static state have been considered.

Users' mobility is a significant feature of wireless communication. By 2030, mobile data traffic will reach close to five zettabytes per month [37], [38], and Cisco anticipates that by 2022, 71% of internet data traffic will be mobile data traffic, over 80% of which will occur indoors [39]. *Great efforts have been made to study the effect of user mobility on the different performances of VLC networks.* For example, [40] theoretically studied the statistical feature of VLC channels under the influence of the random orientation of mobile receivers, and system reliability, such as the bit error rates and outage probability, was derived. Based on a series of experimental measurements, the model of the random orientation of mobile receivers was presented in [41], and the handover rate of a light-fidelity (LiFi) network was assessed for user's random waypoint mobility (RWP) process. Reference [42] presented the statistical characteristics of the SNR for a VLC system where user movement obeyed RWP. Considering the influence of user mobility, channel characteristics were modeled by the ray tracing method and experimental measurements in [43] and [44], respectively. Transmit power allocation subject to the achievable rate constraints of mobile users (MUs) in a VLC network on the basis of NOMA was investigated in [45]. An efficient dynamic association between MUs and optical access points (OAPs) was designed in the presence of user mobility and traffic dynamics in [46]. Power allocation for dynamic association between MUs and OAPs in a cell-free VLC was presented in [47], which was formed into a network utility maximization problem. Although much effort has been made to study user movement, to date, research on its effect on the PLS performance of VLC networks based on NOMA has not been carried on.

B. MOTIVATIONS

To date, studies on PLS for MUs in VLC networks based on NOMA are rare in the open literature. With the fast-developing mobile internet of things (IoTs), whether mobile payments, mobile social networking or mobile offices, security is the primary demand for high user density scenarios in 5G networks and beyond. Hence, it is significant to make research on PLS for MUs in NOMA-enabled VLC networks.

Due to the limitation of the half-power angle of LEDs, mobility will make users move out of the optical attocell dominated by one OAP and migrate into the service area of other OAPs. User mobility will cause an OAP allocation problem and user association with one particular OAP, which is a resource allocation problem. In this paper, such a resource allocation problem will be transformed into the problem of dynamically allocating power, i.e., to dynamically allocate the power of each OAP and to dynamically allocate transmit power based on NOMA among the associated MUs at each OAP. Furthermore, taking external eavesdropping into account, we formulate a joint problem of secure communication and power allocation to maximize the secrecy performance of the network under the constraints of the maximum power of OAPs and power allocation based on NOMA among the associated MUs at each OAP.

This work investigates a VLC network based on downlink NOMA that includes multiple OAPs deployed in the ceiling and multiple MUs moving on the ground. Each OAP serves its associated MUs via NOMA. Every OAP covers an optical attocell. At the edge of each optical attocell, there exists an eavesdropper (Eve) eavesdropping or intercepting the information sent from this OAP to its associated legitimate MUs. Both legitimate MUs and the Eve are assumed to be with a PD receiver. For each OAP, the channel state information (CSI) of MUs associated with this OAP is assumed to be perfectly known. In general, this CSI can be obtained by evaluating at the side of the MU, and it can be fed back to the corresponding OAP via an uplink infrared channel [2]. Since the Eve eavesdrops at the boundary of each optical attocell, and the separation distance between the Eve and the projection of the OAP that the Eve belongs to on the ground holds constant, the propagation distance between the OAP and the Eve can be known. Based on the characteristics of the visible light channel and optical transceiver, the instantaneous CSI of the Eve can be obtained. Note that it is feasible to assume that the Eve is static or moves around the boundary of each optical attocell. For example, the boundary of an optical attocell can be considered the boundary of a protected zone that the Eve cannot enter and is located only at the boundary of the protected zone to wiretap the downlink messages from the OAP to MUs to the maximum extent. Similar assumptions can be seen [33], [48]. This may require authentication and authorization to NOMA legitimate users, which is not the focus of this work and will be covered in the future. In this work, each OAP serves its associated MUs via NOMA, all the signals of MUs associated with one OAP are superposition coded at this OAP, and SIC operation is performed at the side of the MU to decode signals from this OAP. The SIC module is embedded in the PD receiver. SIC can make MUs remove some interuser interference, and it is helpful in expanding the channel difference between legitimate MUs and the eavesdropping channel and, ultimately, in improving network secrecy performance.

C. CONTRIBUTIONS

Specifically, in the following, we list the main contributions:

- In view of the secrecy requirements of VLC and the massive connectivity demand of future communication and considering user movement, this work investigates PLS for MUs in a NOMA-based VLC network. Joint secure communication and power allocation optimization is formulated to maximize the network sum secrecy capacity (NSSC) of MUs in each time frame with the constraint of the maximum power of each OAP and the constraint of power allocation based on NOMA among the associated MUs at each OAP.

- The formulated joint optimization problem is not convex and the optimal solution cannot directly be found. In each time frame, a hierarchical optimization is proposed to maximize the network's NSSC based on the key idea of iterative security-aware water-filling (SWF) and the optimality conditions of Karush-Kuhn-Tucker (KKT). We ultimately find the optimal solution utilizing this hierarchical algorithm. For the proposed NSSC maximization problem considering user movement, the optimal decisions on the power allocation of all OAPs and MUs are made in real time based on the indoor optical wireless channel conditions in each time frame.
- Simulation experiments are performed to illustrate the convergence and effectiveness of the network secrecy performance of the presented power allocation algorithm. Given relevant parameters, decreasing the number of MUs moving in the model room and narrowing the maximum optical beam of the LEDs embedded in the OAPs and the FoV of the PD receiver can improve the NSSC of all legitimate MUs. The NSSC can also be improved by deploying more OAPs in the room.

Notably, the work of this paper is different from that of [35]. First, there are multiple optical attocells in this work, and mobility causes users to move out of the optical attocell dominated by one OAP and migrate into the service area of other OAPs. In contrast, [35] considers only a single optical attocell where the legitimate NOMA users in static state are affected by multiple randomly roaming eavesdroppers modeled as homogeneous Poisson point processes (PPPs). Second, optimization theory is used to find the optimal solution to the joint secure communication and power allocation optimization problem. In contrast, [35] uses stochastic geometry theory to derive the SOP performance of the system based on analyzing the statistical characteristics of the legitimate channel and eavesdropping channel.

The remainder of this work is as follows: Considering user movement, Section II introduces a secure VLC network model with NOMA. In Section III, the joint problem of secure communication and power management is formulated. Section IV presents a hierarchical power allocation algorithm to dynamically allocate OAPs to MUs and to allocate transmit power based on NOMA among the associated MUs at each OAP to maximize the NSSC of the network. In addition, the computing complexity of the algorithm is investigated. Section V performs numerical simulations and obtains the corresponding results. Section VI presents the conclusions.

II. SYSTEM MODEL

The VLC network considered in this work is shown in Figure 1, where $\mathcal{M}=\{1,2,\cdots,M\}$ OAPs are deployed in the ceiling of a room and $\mathcal{N}=\{1,2,\cdots,N\}$ MUs are moving on the ground. Based on the received signal strength, each MU selects one of the OAPs as its associated OAP. Every OAP serves its associated MUs via downlink NOMA,

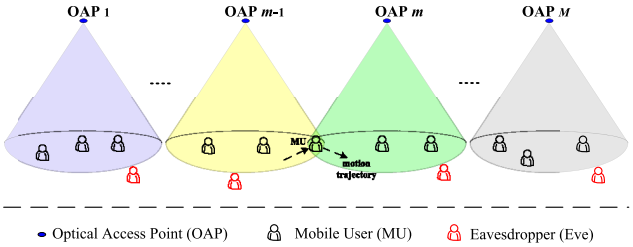


FIGURE 1. NOMA-enabled VLC network with MUs and eavesdroppers.

and each OAP covers an optical attocell with a diameter of approximately 2-3 meters. Thus, the proposed network has M optical attocells. At the edge of each optical attocell, there is an Eve trying to eavesdrop on the information sent from this OAP to its associated legitimate MUs. Each of the legitimate MUs and the Eve are assumed to be equipped with one PD receiver, which has a SIC module.

Let the location of OAP m be $\boldsymbol{x}_m$, and in time frame t, let the location of MU n be $\boldsymbol{y}_{n,t}$; the motion trajectory of MU n can be described as $\{\boldsymbol{y}_{n,t}\}_{t=1,2,\ldots}$. The proposed dynamic VLC network is assumed to be divided into multiple time frames. Information transmission is assumed to be based on a time frame during which each OAP synchronizes the information transmission among all of its associated MUs. The gains of the optical wireless channels in one OAP remain constant over a time frame, and they can vary from one time frame to another due to user movement.

For the proposed secure NOMA-enabled VLC network, the effect of both external eavesdropping and user mobility should be jointly taken into account. Considering user mobility, it is necessary to dynamically allocate resources. Such resource allocation consists of two parts: OAP allocation with the moving of the MUs and the transmit power allocation of each OAP to its associated MUs based on NOMA. Furthermore, taking external eavesdropping into account, it is essential to measure the network's secrecy performance. The NSSC of all legitimate MUs is utilized in this paper.

For this purpose, a secrecy evaluation framework for MUs in a VLC network based on downlink NOMA is proposed in Figure 2. The VLC network consists of two decision-making layers: Layer 1 and Layer 2. At Layer 2, the OAPs serve MUs through optical wireless channels on the basis of NOMA. The allocation of transmit power based on NOMA to each OAP's associated MUs and the determination of the SIC order are performed at this layer. At Layer 1, the allocation of OAPs and the maximization of network secrecy performance subject to the resource allocation constraint are determined. Implementation is explained in detail in Section IV. Finally, the derived results are fed back to the optical control center (OCC), which is connected to all OAPs via a power line or optical fiber.

III. JOINT OPTIMIZATION OF SECURE COMMUNICATION AND POWER ALLOCATION

In this paper, we assume that in time frame t, OAP m has a power of $P_{m,t}$, which is utilized to transmit information to all

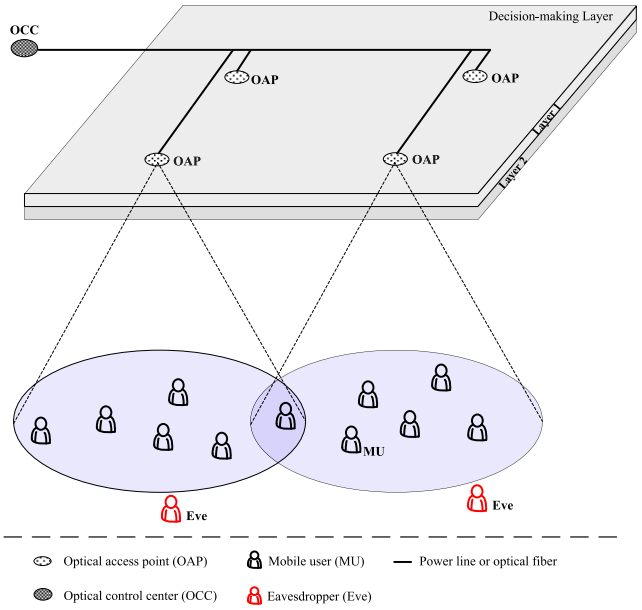


FIGURE 2. A secrecy evaluation framework for MUs in a VLC network based on downlink NOMA.

MUs associated with this OAP, with its maximum achievable value being $P_{m,\max}$. Based on the downlink NOMA scheme, OAP m allocates the transmit power of $p_{m,n,t}$ to MU n, which is a user associated with OAP m in time frame t.

Owing to user mobility, whether OAP m is active (serving users) or idle (not serving users) in time frame t can be determined by

$$\begin{cases} P_{m,t} > 0, & \text{OAP } m \text{ is serving users} \\ P_{m,t} = 0, & \text{OAP } m \text{ is not servingusers} \end{cases} \tag{1}$$

Additionally, whether or not MU n is a user associated with OAP m in time frame t can be determined by

$$\begin{cases} p_{m,n,t} > 0, & \text{MU } n \text{ is user association with OAP } m \\ p_{m,n,t} = 0, & \text{MU } n \text{ is not user association with OAP } m \end{cases} \tag{2}$$

Thus, the resource allocation problem due to the mobility of users can be transformed into a power allocation problem that consists of dynamically adjusting the total power of each OAP and allocating the transmit power based on NOMA among the associated MUs at each OAP.

Furthermore, taking external eavesdropping into account, we ultimately formulate the problem of secure communication and power allocation optimization. This joint problem consists of maximizing the NSSC of all legitimate MUs in each time frame with the constraint of the maximum power of each OAP and the constraint of power allocation based on NOMA among the associated MUs at each OAP.

A. SIGNAL-TO-INTERFERENCE-PLUS-NOISE RATIO (SINR) OF MUs AND THE EVE

In general, information propagation from the OAP to the PD receiver may be in the LoS or diffuse path. Note that Zeng *et al.* pointed out the strongest diffuse part is far less than the weakest LoS [49]. Thus, here, we consider only the LoS path. Assume that white LEDs work in a generalized Lambertian radiation pattern and that in time frame t, the LoS channel gain of the optical wireless channel between OAP m and MU n is $h_{m,n,t}$, which can be written as $h_{m,n,t} = S\rho\,(j+1)\cos^{j}(\phi_m)\cos(\varphi_n)/(2\pi\left\|\boldsymbol{y}_{n,t}-\boldsymbol{x}_m\right\|^2)$, where ρ is the PD receiver's responsivity, j is the Lambertian radiation order, and S is the PD receiver's area. ϕ_m is the radiation angle of the LED at OAP m, and φ_n is the incident angle of the PD at MU n, where ϕ_m is restricted to take a value within the half-power angle and φ_n must be confined to the FoV of the PD. $\left\|\boldsymbol{y}_{n,t}-\boldsymbol{x}_m\right\|$ is the spatial distance between OAP m and MU n.

In practical VLC networks, since the coverage range of adjacent OAPs overlaps, if MUs move close to the edge of each optical attocell, they will suffer from interattocell interference. If in time frame t MU n is a user associated with OAP m, then the interattocell interference $\mathrm{I}'_{m,n,t}$ suffered by MU n associated with OAP m is given by

$$\mathrm{I}'_{m,n,t} = \sum_{m'\in\mathcal{M}\setminus\{m\}} h_{m',n,t}P_{m',t} \tag{3}$$

where $\mathcal{M}\setminus\{m\}$ represents the set $\mathcal{M}$ of all indoor OAPs other than OAP m.

Therefore the real-time CSI of MU n associated with OAP m can be described by

$$\tilde{h}_{m,n,t} = \frac{h_{m,n,t}}{\mathrm{I}'_{m,n,t}+\sigma_n} \tag{4}$$

where σ_n is the received noise power at MU n.

We assume that the feasible set of MUs associated with OAP m in time frame t is $\mathcal{K}_{m,t}$, with $\left|\mathcal{K}_{m,t}\right|$ being its maximum value. Each MU chooses OAP m as an associated OAP in accordance with the strength of the pilot signal. OAP m serves all of its associated MUs based on downlink NOMA. The $\left|\mathcal{K}_{m,t}\right|$ signals are superposition coded at OAP m. The PD receiver of MU n utilizes the SIC module to decode the received signals from OAP m. Without loss of generality, the SIC order for all the MUs associated with OAP m is assumed to be in an increasing order of $\tilde{h}_{m,n,t}$ for all $n\in K_{m,t}$. Therefore, MU n first decodes the received signals with a lower order of interference cancellation than MU n and then treats the received signals with a higher order of interference cancellation than MU n as interference. In this way, in time frame t, the SINR of MU n associated with OAP m can be given by

$$Q_{m,n,t} = \frac{p_{m,n,t}\tilde{h}_{m,n,t}}{\sum\limits_{\forall n'\in\mathcal{K}_{m,t}:\tilde{h}_{m,n',t}>\tilde{h}_{m,n,t}} p_{m,n',t}\tilde{h}_{m,n,t}+1} \tag{5}$$

where $n'\in\mathcal{K}_{m,t}:\tilde{h}_{m,n',t}>\tilde{h}_{m,n,t}$ means that for any MU $n'\in\mathcal{K}_{m,t}$, its optical wireless channel gain $\tilde{h}_{m,n',t}$ is larger than that of MU n, which is expressed by $\tilde{h}_{m,n,t}$.

Since the Eve eavesdrops at the boundary of each optical attocell, the spatial distance between the Eve and its belonging to the OAP holds constant (the Eve can be static or move around the boundary of each optical attocell). With $h_{m,e,t}$ being the instantaneous CSI of the Eve associated with OAP m in time frame t, the SINR of the Eve eavesdropping on MU n associated with OAP m in time frame t is

$$Q_{m,e\to n,t} = \frac{p_{m,n,t}h_{m,e,t}}{\sum\limits_{\forall n'\in\mathcal{K}_{m,t}:\tilde{h}_{m,n',t}>\tilde{h}_{m,n,t}} p_{m,n',t}h_{m,e,t}+1} \tag{6}$$

B. NSSC MAXIMIZATION

In time frame t, the secrecy capacity [50] of MU n associated with OAP m can be written as

$$C_{m,n,t} = \left[\log\left(1+Q_{m,n,t}\right) - \log\left(1+Q_{m,e\to n,t}\right)\right]^{+} \tag{7}$$

The sum secrecy capacity of all the legitimate MUs associated with OAP m can be described by

$$C_{m,t} = \sum_{\forall n\in\mathcal{K}_{m,t}} C_{m,n,t} \tag{8}$$

The NSSC of all the legitimate MUs within all OAPs can be expressed as

$$C_t = \sum_{\forall m\in\mathcal{M}} C_{m,t} \tag{9}$$

In summary, the joint secure communication and power allocation optimization problem for a NOMA-enabled VLC network in the case of external eavesdropping and user mobility can be described by

$$\max_{\substack{\{P_{m,t}|m\in\mathcal{M}\}\\ \{p_{m,n,t}|n\in\mathcal{K}_{m,t}\ for\ \forall m\in\mathcal{M}\}}} \quad C_t \tag{10-1}$$

$$\text{s.t. } 0 \le P_{m,t} \le P_{m,\max}, \quad \forall m \tag{10-2}$$

$$\sum_{\forall n\in\mathcal{K}_{m,t}} p_{m,n,t} \le P_{m,t}, \quad \forall m \tag{10-3}$$

$$P_{m,t}\ge 0, p_{m,n,t}\ge 0, \quad \forall m,n. \tag{10-4}$$

where (10-2) is the total power constraint of OAP m in time frame t, with its value $P_{m,t}$ not being larger than $P_{m,\max}$ and (10-3) is the power allocation constraint where OAP m allocates power to all of its associated MUs based on NOMA.

It is obvious from (10) that maximizing NSSC C_t through the optimization of variables $P_{m,t}$ and $p_{m,n,t}$ for all m and n is a nonconvex optimization problem because there is a logarithmic subtraction operation in the objective function. Therefore, we cannot directly determine the optimal solution via convex optimization theory. Notably, however, in the joint optimization problem of (10), there are two kinds of power allocation: for each OAP and for the associated MUs at each OAP. Thus, we can separately allocate the total power of each OAP and the transmit power of each OAP to MUs.

In the following, a hierarchical power allocation algorithm is naturally proposed; it is performed at the proposed decision-making layer. At Layer 1, the optimal total power of each OAP is determined. At Layer 2, the optimal transmit power of each OAP to its associated MUs based on NOMA is determined.

IV. HIERARCHICAL POWER ALLOCATION ALGORITHM

The NSSC maximization problem subject to the power allocation constraints can be solved in two successive phases. First, when the power allocation among OAPs is given, the power allocation algorithm is performed at each OAP to obtain the optimal power allocation to MUs that are users associated with a certain OAP. Then, in view of the feedback of the power allocation to MUs based on NOMA, the optimal power allocation among OAPs is determined to maximize the NSSC.

A. POWER ALLOCATION SUBPROBLEM AT LAYER 2

In this subsection, assume that the power allocation among OAPs is given, and the NOMA-based optimal power allocation of each OAP to its associated MUs is derived.

In particular, if the total power $P_{m,t}$ of OAP m has been given, then the joint optimization problem (10) of secure communication and power allocation can be described by

$$\max_{\{p_{m,n,t}|n\in\mathcal{K}_{m,t}\ for\ \forall m\in\mathcal{M}\}} C_{m,t} = \sum_{\forall n\in\mathcal{K}_{m,t}} C_{m,n,t}$$
$$\text{s.t.} \sum_{\forall n\in\mathcal{K}_{m,t}} p_{m,n,t} \le P_{m,t}, \quad \forall m$$
$$p_{m,n,t}\ge 0, \quad \forall m,n. \tag{11}$$

From (11), the sum secrecy capacity of all legitimate NOMA MUs associated with OAP m is maximized by adjusting the transmit power of OAP m to all of its associated MUs.

Lemma 1: If the total power of all OAPs deployed in the room has been given, the maximization problem of the sum secrecy capacity in (11) can be transformed into a problem of convex optimization.

Proof: From (7) we know that $C_{m,n,t} = \max\left\{\log\left(1+Q_{m,n,t}\right) - \log\left(1+Q_{m,e\to n,t}\right), 0\right\}$, thus, when $Q_{m,n,t} < Q_{m,e\to n,t}$, $C_{m,n,t} = 0$.

The OAP can be assumed to obtain the CSI of all MUs and the Eve associated with OAP m in time frame t, and furthermore, it can feedback the CSI to the MUs, during which the Eve can also get the CSI. To facilitate further analysis, the SIC order for all MUs and the Eve associated with OAP m in time frame t is assumed to be in an increasing order, i.e.,

$$\tilde{h}_{m,1,t}\le\cdots\le\tilde{h}_{m,N_e,t}\le h_{m,e,t}\le\tilde{h}_{m,N_e+1,t},\le\cdots\le\tilde{h}_{m,|\mathcal{K}_{m,t}|,t},$$

where $\tilde{h}_{m,N_e,t}$ denotes the optical wireless channel gain of the N_e-th MU belonging to set $\mathcal{K}_{m,t}$, while $\left|\mathcal{K}_{m,t}\right|$ refers to the maximum value of the possible set $\mathcal{K}_{m,t}$ of MUs associated with OAP m in time frame t. Thus, for any MU belonging to $N_e+1 \le n \le \left|\mathcal{K}_{m,t}\right|$, the secrecy capacity $C_{m,n,t}$ of MU n within OAP m in time frame t can eliminate nonpositive values. Then, we can rearrange the objective function in

problem (11) as

$$C_{m,t} = \sum_{n=1}^{|\mathcal{K}_{m,t}|} \left[\log\left(1+Q_{m,n,t}\right) - \log\left(1+Q_{m,e\to n,t}\right)\right]^{+} \tag{12-1}$$

$$= \sum_{n=N_e+1}^{|\mathcal{K}_{m,t}|} \log\left(\frac{1+Q_{m,n,t}}{1+Q_{m,e\to n,t}}\right) \tag{12-2}$$

$$= \sum_{n=N_e+1}^{|\mathcal{K}_{m,t}|} \left[\log \frac{\tilde{h}_{m,n,t}\sum_{i=n}^{|\mathcal{K}_{m,t}|} p_{m,i,t}+1}{\tilde{h}_{m,n,t}\sum_{i=n+1}^{|\mathcal{K}_{m,t}|} p_{m,i,t}+1} - \log \frac{h_{m,e,t}\sum_{i=n}^{|\mathcal{K}_{m,t}|} p_{m,i,t}+1}{h_{m,e,t}\sum_{i=n+1}^{|\mathcal{K}_{m,t}|} p_{m,i,t}+1}\right] \tag{12-3}$$

where (12-2) holds by utilizing the increasing order of SIC, and (12-3) follows from substituting (5) and (6) into (12-2).

It is easy to transform the first term in (12-3) into

$$\sum_{n=N_e+1}^{|\mathcal{K}_{m,t}|} \log \frac{\tilde{h}_{m,n,t}\sum_{i=n}^{|\mathcal{K}_{m,t}|} p_{m,i,t}+1}{\tilde{h}_{m,n,t}\sum_{i=n+1}^{|\mathcal{K}_{m,t}|} p_{m,i,t}+1}$$
$$= \log\left(\tilde{h}_{m,N_e+1,t}\left(\sum_{i=N_e+1}^{|\mathcal{K}_{m,t}|} p_{m,i,t}\right)+1\right)$$
$$+ \sum_{n=N_e+1}^{|\mathcal{K}_{m,t}|-1}\left[\log\left(\tilde{h}_{m,n+1,t}\left(\sum_{i=n+1}^{|\mathcal{K}_{m,t}|} p_{m,i,t}\right)+1\right) - \log\left(\tilde{h}_{m,n,t}\left(\sum_{i=n+1}^{|\mathcal{K}_{m,1}|} p_{m,i,t}\right)+1\right)\right] \tag{13}$$

and to transform the second term in (12-3) into

$$\sum_{n=N_e+1}^{|\mathcal{K}_{m,t}|} \log \frac{h_{m,e,t}\sum_{i=n}^{|\mathcal{K}_{m,t}|} p_{m,i,t}+1}{h_{m,e,t}\sum_{i=n+1}^{|\mathcal{K}_{m,t}|} p_{m,i,t}+1} = \log\left(h_{m,e,t}\left(\sum_{i=N_e+1}^{|\mathcal{K}_{m,t}|} p_{m,i,t}\right)+1\right) \tag{14}$$

If we define

$$\psi_{n,t} \triangleq \begin{cases} h_{m,e,t}, & n = N_e \\ \tilde{h}_{m,n,t}, & N_e+1 \le n \le |\mathcal{K}_{m,t}| \end{cases} \tag{15}$$

$$\zeta_{n,t} \triangleq \sum_{i=n+1}^{|\mathcal{K}_{m,t}|} p_{m,i,t}, \quad N_e \le n \le |\mathcal{K}_{m,t}|-1 \tag{16}$$

$$f\left(\zeta_{n,t}\right) = \log\left(\psi_{n+1,t}\zeta_{n,t}+1\right) - \log\left(\psi_{n,t}\zeta_{n,t}+1\right) \tag{17}$$

then (12) can be transformed into

$$C_{m,t} = \sum_{n=N_e}^{|\mathcal{K}_{m,t}|-1} f\left(\zeta_{n,t}\right) \tag{18}$$

It is obvious from (18) that the function of $C_{m,t}$ consists of $|\mathcal{K}_{m,t}| - N_e$ subfunctions. That is, problem (11) can be viewed as the sum of $|\mathcal{K}_{m,t}| - N_e$ subproblems, each of which individually maximizes the function of $f\ (\zeta_{n,t})$ for the n-th MU subject to the transmit power constraints on the basis of NOMA. Utilizing the solutions to these subproblems, we can finally get the optimal power allocation to MUs associated with the same OAP.

Particularly for function $f\ (\zeta_{n,t})$ of the n-th MU belonging to $\mathcal{K}_{m,t}$, its first-order derivative on $\zeta_{n,t}$ is

$$\frac{df\left(\zeta_{n,t}\right)}{d\zeta_{n,t}} = \frac{\psi_{n+1,t}}{\psi_{n+1,t}\zeta_{n,t}+1} - \frac{\psi_{n,t}}{\psi_{n,t}\zeta_{n,t}+1} = \frac{\psi_{n+1,t}-\psi_{n,t}}{\left(\psi_{n+1,t}\zeta_{n,t}+1\right)\left(\psi_{n,t}\zeta_{n,t}+1\right)} \tag{19}$$

Because of the increasing order of $\tilde{h}_{m,n,t}$, we can easily get $\psi_{n+1,t} > \psi_{n,t}$, finally we can derive $df\left(\zeta_{n,t}\right)/d\zeta_{n,t} > 0$.

Thus, function $f\ (\zeta_{n,t})$ monotonically increases with parameter $\zeta_{n,t}$; and, the maximization of $f\ (\zeta_{n,t})$ is equivalent to the maximization of $\zeta_{n,t}$. Therefore, the optimization problem (11) is rewritten by

$$\max_{\{p_{m,n,t}|n\in\mathcal{K}_{m,t}\ for\ \forall m\in\mathcal{M}\}} \zeta_{n,t} \tag{20-1}$$

$$\text{s.t.} \sum_{\forall n\in\mathcal{K}_{m,t}} p_{m,n,t} \le P_{m,t}, \quad \forall m \tag{20-2}$$

$$p_{m,n,t} \ge 0, \quad \forall m, n. \tag{20-3}$$

The constraint in (20-2) is obviously convex [51], and the objective function is linear; hence, the optimization problem of (20) is convex. This is the end of the proof and leads to Lemma 1. ■

Next, given the total power $P_{m,t}$ of OAP m and based on NOMA, the optimal power allocation to all of the MUs associated with OAP m (the optimal solutions to problem (20) and, hence, problem (11)) is presented by using the results of Lemma 1.

Theorem 1: The total power of optical access point m in time frame t should be greedily assigned to the mobile user which has the highest optical wireless channel gain, so as to maximize the sum secrecy capacity across all mobile users associated with m.

Proof: By substituting (16) into (20-1), we can obtain the corresponding Lagrangian function of (20), which is

$$J\left(p_{m,n,t}, \beta, \{\alpha_n\}\right) = \sum_{i=n+1}^{|\mathcal{K}_{m,t}|} p_{m,i,t} + \beta\left\{P_{m,t} - \sum_{n=1}^{|\mathcal{K}_{m,t}|} p_{m,n,t}\right\} + \sum_{n=1}^{|\mathcal{K}_{m,t}|} \alpha_n p_{m,n,t} \tag{21}$$

where β and α_n are the Lagrangian multipliers for constraints (20-2) and (20-3), respectively. According to the KKT conditions, the following should be satisfied:

$$\frac{\partial J(\cdot)}{\partial p_{m,n,t}} = -\beta + \alpha_n = 0,\ N_e \le n \le \left|\mathcal{K}_{m,t}\right| - 1 \quad (22\text{-}1)$$

$$\sum_{n=1}^{|\mathcal{K}_{m,t}|} p_{m,n,t} = P_{m,t} \quad (22\text{-}2)$$

$$\alpha_n p_{m,n,t} = 0, \quad N_e \le n \le \left|\mathcal{K}_{m,t}\right| - 1 \quad (22\text{-}3)$$

From (21) and (22-1), we can get

$$\frac{\partial J(\cdot)}{\partial p_{m,n+1,t}} = 1 - \beta + \alpha_{n+1} = \alpha_{n+1} - \alpha_n + 1 = 0,\ N_e \le n \le \left|\mathcal{K}_{m,t}\right| - 1 \quad (23)$$

It is easily deduced from (23) that $\alpha_{|\mathcal{K}_{m,t}|} = 0$ and $\alpha_n > 0$ for all $N_e \le n \le \left|\mathcal{K}_{m,t}\right| - 1$. Thus, the implication of (22-2) and (22-3) is that OAP m serves only its associated $\left|K_{m,t}\right|$-th MU belonging to $K_{m,t}$, i.e., the MU with the best optical wireless channel gain, with all of its power $P_{m,t}$. The proof ends here, and Theorem 1 follows. ■

According to Theorem 1, the primary work of OAP m consists of determining the associated optimal mobile user $n^*_{m,t}$ that has the highest optical wireless channel gain $\tilde{h}_{m,n,t}$, i.e.,

$$n^*_{m,t} = \arg\max_{\forall n \in \mathcal{K}_{m,t}} \tilde{h}_{m,n,t} = \arg\max_{\forall n \in \mathcal{K}_{m,t}} \frac{h_{m,n,t}}{\sum_{m' \in \mathcal{M}\setminus\{m\}} h_{m',n,t} P_{m',t} + \sigma_n} \quad (24)$$

and the secondary work consists of assigning the total power $P_{m,t}$ of OAP m to its associated optimal mobile user $n^*_{m,t}$ in time frame t.

B. POWER ALLOCATION SUBPROBLEM AT LAYER 1

In this subsection, in view of the feedback of power allocation among MUs at Layer 2, the optimal power allocation among OAPs is determined in order to maximize the NSSC.

By Theorem 1, the NSSC maximization problem with respect to the power allocation constraints in each time frame t can be rearranged as

$$\begin{aligned}
&\max_{\{P_{m,}|m\in\mathcal{M}\}} C_t \\
&= \sum_{\forall m\in\mathcal{M}} \left[\log\left(1 + \frac{P_{m,t} h_{m,n^*,t}}{\sum_{\forall m'\in\mathcal{M}\setminus\{m\}} h_{m',n^*,t} P_{m',t} + \sigma_{n^*}}\right) \right. \\
&\quad \left. - \log\left(1 + \frac{P_{m,t} h_{m,e,t}}{\sum_{\forall m'\in\mathcal{M}\setminus\{m\}} h_{m',e,t} P_{m',t} + \sigma_e}\right) \right]^+ \\
&\text{s.t. } 0 \le P_{m,t} \le P_{m,\max}, \quad \forall m \in \mathcal{M} \\
&\quad P_{m,t} \ge 0, \quad \forall m \in \mathcal{M}
\end{aligned} \quad (25)$$

For simplicity, the operation of $[\cdot]^+$ in problem (25) is removed in the following by omitting the OAPs with non-positive secrecy capacity.

Define

$$A_{m,t} \triangleq \frac{1}{h_{m,n^*,t}} \left(\sum_{m'\in\mathcal{M}\setminus\{m\}} h_{m',n^*,t} P_{m',t} + \sigma_{n^*} \right)$$

$$B_{m,t} \triangleq \frac{1}{h_{m,e,t}} \left(\sum_{m'\in\mathcal{M}\setminus\{m\}} h_{m',e,t} P_{m',t} + \sigma_e \right) \quad (26)$$

It can be deduced from (26) that when $A_{m,t} < B_{m,t}$, the operation of $[\cdot]^+$ in the objective function of (25) can be omitted. Then, (25) can be simplified as

$$\begin{aligned}
&\max_{\left\{P_{m,t}|m\in\widetilde{\mathcal{M}}\right\}} C_t = \sum_{\forall m\in\widetilde{\mathcal{M}}} \log\left(\frac{1 + P_{m,t}/A_{m,t}}{1 + P_{m,t}/B_{m,t}}\right) \\
&\text{s.t. } 0 \le P_{m,t} \le P_{m,\max}, \quad \forall m \in \widetilde{\mathcal{M}} \\
&\quad P_{m,t} \ge 0, \quad \forall m \in \widetilde{\mathcal{M}}
\end{aligned} \quad (27)$$

where $\widetilde{\mathcal{M}} = \left\{ m \in \mathcal{M} | A_{m,t} < B_{m,t} \right\}$ denotes the set of OAPs in which positive secrecy capacity can be obtained. Obviously the OAPs in $\mathcal{M}\setminus\widetilde{\mathcal{M}}$ are treated as unavailable nodes, and not any power is allocated to them.

From (27), the NSSC maximization problem involves the maximization of the secrecy capacity of each OAP for $m \in \widetilde{\mathcal{M}}$, which can be regarded as a noncooperative game problem where the players are concerned with only their own secrecy performance according to game theory [52].

In the following, we first apply a noncooperative secrecy competition game to model the NSSC maximization problem in a distributed manner. Then, Nash equilibrium is utilized to characterize the steady states of the proposed noncooperative game. Next, an equivalent variational inequality (VI) is leveraged for the equilibrium. Finally, by using the equivalence of the noncooperative game and the VI problem, we derive the optimal power allocation algorithm for each OAP.

In time frame t, there exists $\mathcal{P}_t = \left\{ P_{m,t} \middle| 0 \le P_{m,t} \le P_{m,\max}, \forall m \in \widetilde{\mathcal{M}} \right\}$; then, problem (27) can be characterized as

$$\begin{aligned}
&\max_{\left\{P_{m,t}|m\in\widetilde{\mathcal{M}}\right\}} C_t = \sum_{\forall m\in\widetilde{\mathcal{M}}} \log\left(\frac{1 + P_{m,t}/A_{m,t}}{1 + P_{m,t}/B_{m,t}}\right) \\
&\text{s.t. } P_{m,t} \in \mathcal{P}_t
\end{aligned} \quad (28)$$

Define $\mathbf{P}_{-m,t} = \{P_{1,t},\ldots,P_{m-1,t},P_{m+1,t},\ldots,P_{M,t}\}$ as the power vector of OAPs not including OAP m. Then, problem (28) is given by

$$\begin{aligned}
&\max_{\left\{P_{m,t}|m\in\widetilde{\mathcal{M}}\right\}} C_t\left(P_{m,t}, \mathbf{P}_{-m,t}\right) \\
&\text{s.t. } P_{m,t} \in \mathcal{P}_t
\end{aligned} \quad (29)$$

Considering that problem (29) should be solved at each individual OAP, this subsection introduces the following noncooperative game, which is described as

$$\mathcal{G}_t = \left\{ \widetilde{\mathcal{M}}, \left\{P_{m,t}\right\}_{m\in\widetilde{\mathcal{M}}}, C_{m,t}\big|_{m\in\widetilde{\mathcal{M}}} \right\} \quad (30)$$

where the OAPs belonging to $\widetilde{\mathcal{M}}$ are as players of the game $\mathcal{G}_t$ to make the secrecy capacity maximization by striving for their respective power.

The steady state of the noncooperative game proposed above can be described by Nash equilibrium. When the network is in such a state, no optical access point can unilaterally deviate from the current equilibrium strategy in order to make a further improvement of its secrecy capacity.

With power allocation strategy profile $\mathbf{P}_t^* = \left[P_{m,t}^*\right]_{m\in\widetilde{\mathcal{M}}}$ at Layer 1, for all the OAPs in $m \in \widetilde{\mathcal{M}}$, the following inequality is always satisfied

$$C_t\left(P_{m,t}^*, \mathbf{P}_{-m,t}^*\right) \geq C_t\left(P_{m,t}, \mathbf{P}_{-m,t}^*\right), \quad \forall P_{m,t} \in \mathcal{P}_t \tag{31}$$

The gradient of $C_t(\mathbf{P}_t)$ with respect to $P_{m,t}$ can be expressed as

$$\nabla_{P_{m,t}} C_t\left(\mathbf{P}_t\right) = \frac{h_{m,n^*,t}}{\sum\limits_{m\in\widetilde{\mathcal{M}}} h_{m,n^*,t}P_{m,t} + \sigma_{n^*}} - \frac{h_{m,e,t}}{\sum\limits_{m\in\widetilde{\mathcal{M}}} h_{m,e,t}P_{m,t} + \sigma_e} \tag{32}$$

Then, for OAP m to be in Nash equilibrium, its first-order optimality condition is expressed as

$$\left(P_{m,t} - P_{m,t}^*\right)\mathbf{F}_t \geq 0 \quad \forall P_{m,t} \in \mathcal{P}_t \tag{33}$$

with $\mathbf{F}_t = -\nabla_{P_{m,t}} C_t\left(\mathbf{P}_t\right)$.

For problem (33), it can be rewritten as a variational inequality $\mathrm{VI}\left(\mathcal{P}_t, \mathbf{F}_t\right)$, where $\mathbf{F}_t$ is the operator and $\mathcal{P}_t$ denotes the feasible set.

Applying the equivalence of the noncooperative game and the VI problem [53, Theorem 1 and Theorem 2], we obtain the corresponding Lagrangian function of (28):

$$J\left(P_{m,t}, \chi_{m,t}\right) = \sum_{\forall m\in\widetilde{\mathcal{M}}} \log\left(\frac{1 + P_{m,t}/A_{m,t}}{1 + P_{m,t}/B_{m,t}}\right) + \chi_{m,t}\left(P_{m,\max} - P_{m,t}\right) \tag{34}$$

with $\chi_{m,t}$ as the Lagrange factor.

In accordance with the KKT conditions, the optimal solution to (28) should satisfy

$$\frac{\partial J\left(P_{m,t}, \chi_{m,t}\right)}{\partial P_{m,t}} = \frac{1}{1+P_{m,t}/A_{m,t}}\frac{1}{A_{m,t}} - \frac{1}{1+P_{m,t}/B_{m,t}}\frac{1}{B_{m,t}} - \chi_{m,t} = 0 \tag{35}$$

Then in time frame t at OAP m, the optimal power allocation with respect to problem (28) is given by

$$P_{m,t} = \frac{1}{2}\max\left\{-\left(A_{m,t} + B_{m,t}\right) + \sqrt{\left(A_{m,t}+B_{m,t}\right)^2 - 4\left(A_{m,t}-B_{m,t}\right)/\chi_{m,t} - 4A_{m,t}B_{m,t}}, 0\right\} \tag{36}$$

which satisfies $0 \leq P_{m,t}^* \leq P_{m,\max}$.

Algorithm 1 The Iterative Algorithm in Each Time Frame to Allocate Power to Each OAP at Layer 1

1 initialization: Let the number of iteration $i = 0$, randomly choose a power allocation for all OAPs $\mathbf{P}(i)$.
2 Based on $A_{m,t} < B_{m,t}$, determine the feasible set $\widetilde{\mathcal{M}}$ of indoor OAPs where positive secrecy capacity can be obtained.
3 repeat
4 for $\forall m \in \widetilde{\mathcal{M}}$ do
5 $P_{m,t}^*(i) = \mathrm{SWF}(\chi_{m,t}(i), \mathbf{P}_{-m,t}^*(i))$
6 $i = i + 1$;
7 until $\|\mathbf{P}_t(i) - \mathbf{P}_t(i-1)\|_2 / \|\mathbf{P}_t(i-1)\|_2 < \varepsilon$, where ε is an arbitrarily small positive constant as the predefined threshold to terminate the iteration process.
8 output: $\mathbf{P}_t(i)$ represents the optimal power allocation for all OAPs in time frame t.

TABLE 1. Simulation parameters.

Parameter	value
Half power angle (θ)	30^0~70^0
Maximum power of each OAP	40W
PD receiver's responsivity	0.4 mA/mW
Room size	10 m×10 m×5 m
physical area of PD receiver	1 cm^2
Time frame length	1ms

Based on the critical idea of the SWF algorithm [53], the solution to the proposed noncooperative secrecy competition game is

$$P_{m,t}^* = \mathrm{SWF}\left(\chi_{m,t}, \mathbf{P}_{-m,t}^*\right), \quad \forall m \in \widetilde{\mathcal{M}} \tag{37}$$

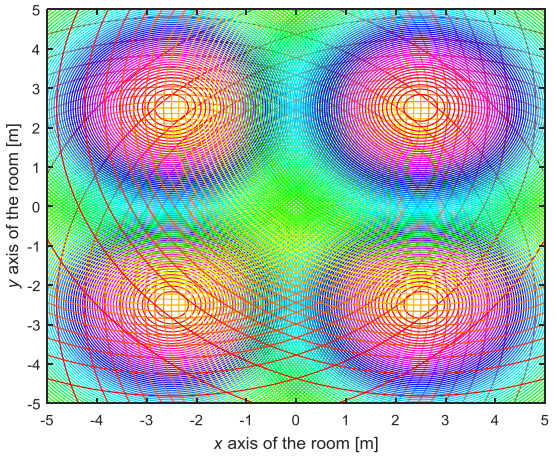
In summary, the power allocation to each OAP at Layer 1 can be described by Algorithm 1.

C. COMPUTATIONAL COMPLEXITY ANALYSIS

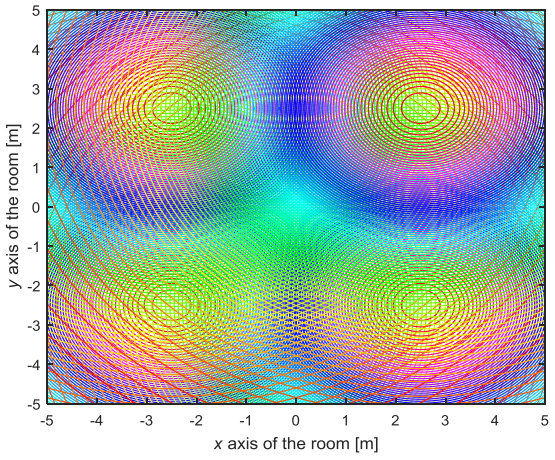
Since the primary work at Layer 2 (shown in (24)) consists of determining the mobile user with the best channel gain for each OAP in each time frame, the computing complexity at Layer 2 is $\mathcal{O}\left(\sum_{m=1}^{M}\left|\mathcal{K}_{m,t}\right|\left(\left|\mathcal{K}_{m,t}\right|-1\right)/2\right)$. The complexity of solving (27) at Layer 1 is $\mathcal{O}\left(M^2(M+1)\right)$, which is obtained by the same approach as [32]. Therefore, the complexity of the proposed hierarchical power allocation algorithm in the paper is $\mathcal{O}\left(M^2(M+1)\sum_{m=1}^{M}\left(\left|\mathcal{K}_{m,t}\right|\left(\left|\mathcal{K}_{m,t}\right|-1\right)/2\right)\right)$.

V. NUMERICAL SIMULATIONS AND RESULTS

In this section, simulation experiments are performed to show the network secrecy performance and to illustrate the convergence and effectiveness of the power allocation algorithm proposed above. The simulation parameters for the room model, PD receiver, LED transmitter, etc. are listed in Table 1.



(a)



(b)

FIGURE 3. The luminous intensity of the four OAPs with the half-power angle. (a) The half-power angle is 30°. (b) The half-power angle is 50°.

In this section, a 10 m×10 m×5 m model room, where four OAPs are deployed in the ceiling and multiple MUs move on the ground, is used. With the room center being the ordinate origin, the four OAPs are located at [−2.5, 2.5, 5], [−2.5, −2.5, 5], [2.5, 2.5, 5], and [2.5, −2.5, 5]. The luminous intensity distributions of the four OAPs with different half-power angles are shown in Figure 3, from which we know that when the half-power angle is 30°, the coverage areas of different OAPs slightly overlap with each other, as shown in Figure 3 (a). However, when we augment the half-power angle, as shown in Figure 3 (b), i.e., let it be 50°, the overlapping coverage range of each OAP also increases.

Since the coherence time for VLC networks is in the order of tens of milliseconds [2], in the simulation process, the length of the time frame is assumed to be 1 ms, which is far less than the coherence time. Therefore, the proposed dynamic VLC network can be divided into multiple time frames, during each of which the CSI of the VLC channel remains constant or changes relatively slowly. Additionally, this means that for every time frame, the two decision-making layers are allowed to dynamically update the OAP

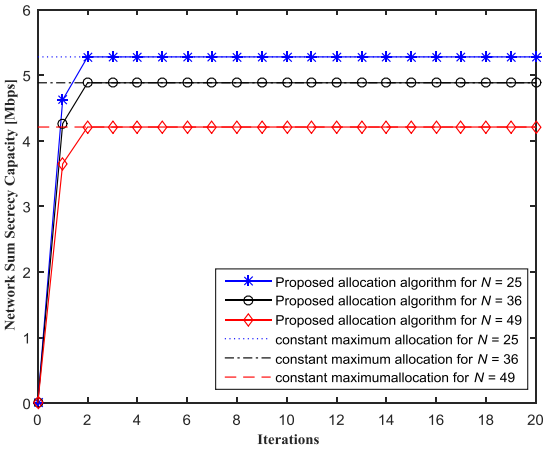


FIGURE 4. Convergence and optimality of the NSSC based on the proposed iterative algorithm.

allocation and the user association situation by the proposed power allocation algorithm. Note that it is possible to perform the dynamic updating per millisecond, because if the two decision-making layers are equipped with cloud computing server, then the computing delay can be controlled in the order of millisecond [54].

First, we investigate the convergence of the iterative algorithm proposed above in Figure 4 with error tolerance $\varepsilon = 10^{-9}$ for various user densities of the legitimate MUs. For purposes of comparison, we also obtain the constant maximum power allocation of each OAP to its associated MUs. Figure 4 shows that the proposed iterative algorithm reaches a steady state within approximately 2 iterations, i.e., a fast convergence can be achieved by the proposed power allocation algorithm, which implies that it is feasible to update the OAP allocation and the user association situation within a millisecond-order time scale. And the NSSC obtained by the proposed iterative algorithm is very close to that derived by the constant maximum power allocation algorithm, which demonstrates the optimality of the proposed iterative algorithm. Additionally, by increasing the number of legitimate MUs, the NSSC of all legitimate MUs worsens. The reason is that the density of MUs in each optical attocell increases with the increase in the number of legitimate MUs moving on the ground, which makes the interattocell interference severe and thus worsens the NSSC.

When the number of legitimate MUs is constant, changing the semiangle of the LED embedded in the OAP at half illuminance will have a great effect on the NSSC. Figure 5 illustrates the effect of the half-power angle on the NSSC, showing that the NSSC performance improves with the decrease in the half-power angle. This result is mainly because the narrowing of the optical beam of the LED will greatly suppress the interattocell interference; thus, the network secrecy performance can be improved.

In the following, given the LED's half-power angle (θ =30°), we investigate the relationship between the PD's FoV and the NSSC. Figure 6 shows that employing a PD receiver with a larger FoV will cause the NSSC to worsen.

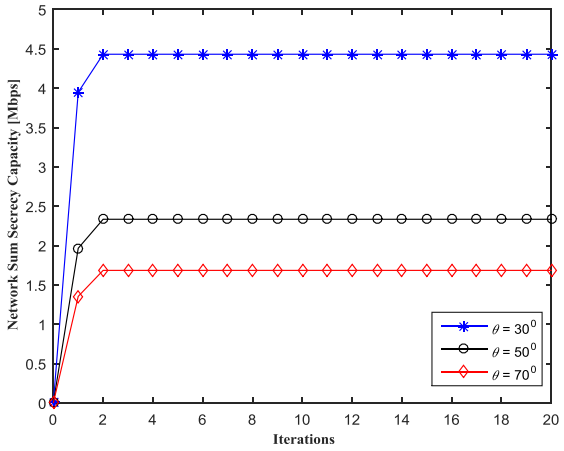


FIGURE 5. The effect of the half-power angle on the NSSC under PD FoV=30°.

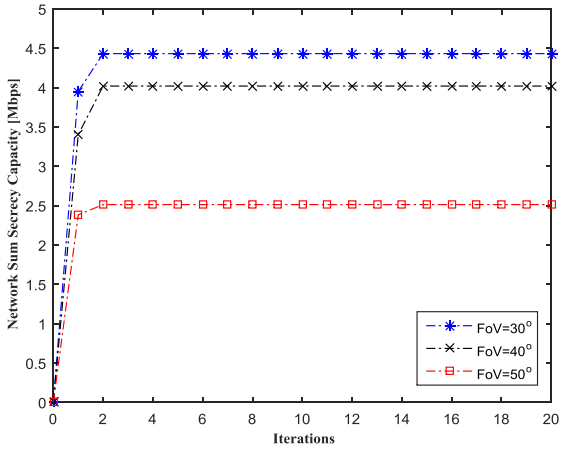


FIGURE 6. The effect of FoV on the NSSC under LED half-power angle $\theta = 30°$.

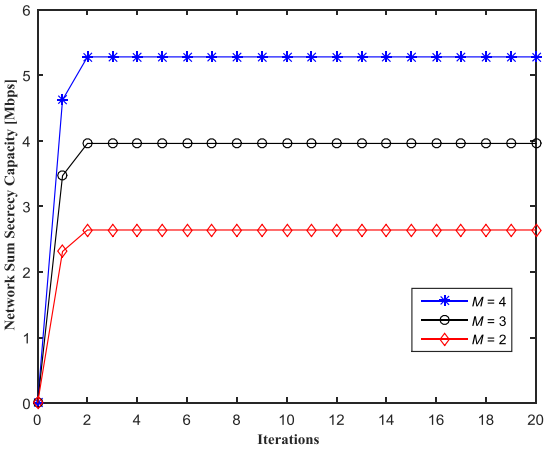


FIGURE 7. The NSSC versus the number of OAPs deployed in the room ceiling under LED half-power angle $\theta = 30°$, PD FoV=30°, and a constant density of MUs.

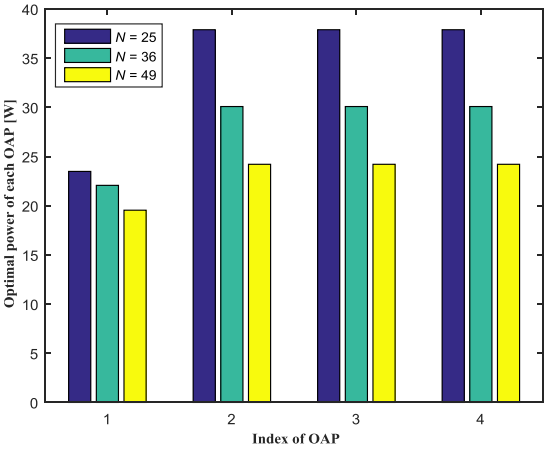


FIGURE 8. Optimal power allocation of four OAPs deployed in the ceiling.

This result is mainly because when the maximum light beam (dependent on the LED's half-power angle) is given, with the increase in the FoV, more noise will enter the PD's receiver, and the interattocell interference will become severe; thus, the network secrecy performance will deteriorate.

Now, we consider the effect of the number of OAPs deployed in the room. The LED's half-power angle and the PD's FoV are all set to 30°, and the density of MUs is held constant ($N = 25$). The first two, the first three and the first four OAPs of the four OAPs mentioned above are employed. Figure 7 shows that the greater the number of OAPs employed, the better the NSSC. This result implies that to improve the network secrecy performance, it is essential to deploy more OAPs in the room ceiling.

Figure 8 shows the optimal power allocation of four OAPs deployed in the ceiling under different densities of MUs. Increasing the number of MUs causes the optimal power allocated to each OAP to decrease. On the one hand, increasing the density of MUs will make the interattocell interference become severe, and thus, the CSI of the legitimate channel will deteriorate. On the other hand, the Eve is static or moves around the boundary of each optical attocell, and the CSI of the Eve holds constant. By reducing the power of the OAP experiencing severe cochannel interference, it is possible to greatly improve the NSSC.

VI. CONCLUSION

The PLS of MUs for a NOMA-enabled VLC network is investigated to meet the massive connectivity demand of future communication and the security demand of VLC. Due to user movement and the dynamic indoor environment, it is necessary to dynamically allocate OAPs and to transmit power to MUs based on NOMA. When MUs are mobile, whether or not an MU is a user associated with a OAP can be determined by whether or not the OAP is active or idle and whether or not power is transmitted to this MU based on NOMA at the OAP if this OAP is active. Therefore, the problem of user association when users are mobile can be transformed into a power allocation problem to dynamically adjust the total power of each OAP and the power based on NOMA among the associated MUs at each OAP. Furthermore, taking external eavesdropping into account, we ultimately formulate a joint secure communication and power allocation optimization problem to maximize the NSSC of MUs in each time

frame. A hierarchical power allocation algorithm is proposed based on the KKT optimality conditions and the approach of the iterative SWF. Simulations of the proposed algorithms are conducted to demonstrate the convergence and effectiveness of the algorithms. The simulation results also show that the NSSC depends on the user density of MUs, the half-power angle of the LED, the FoV of the PD and the number of OAPs deployed in the model room.

REFERENCES

[1] T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights," *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 100–107, Feb. 2004.

[2] Z. Zeng, M. Dehghani Soltani, Y. Wang, X. Wu, and H. Haas, "Realistic indoor hybrid WiFi and OFDMA-based LiFi networks," *IEEE Trans. Commun.*, vol. 68, no. 5, pp. 2978–2991, May 2020.

[3] N. Kumar, D. Terra, N. Lourenco, L. Nero Alves, and R. L. Aguiar, "Visible light communication for intelligent transportation in road safety applications," in *Proc. 7th Int. Wireless Commun. Mobile Comput. Conf.*, Istanbul, Turkey, Jul. 2011, pp. 1513–1518.

[4] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May 2020.

[5] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[6] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5G," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2294–2323, 3rd Quart., 2018.

[7] L. P. Qian, Y. Wu, H. Zhou, and X. Shen, "Dynamic cell association for non-orthogonal multiple-access V2S networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2342–2356, Oct. 2017.

[8] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[9] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[10] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[11] H. Marshoud, V. M. Kapinas, G. K. Karagiannidis, and S. Muhaidat, "Non-orthogonal multiple access for visible light communications," *IEEE Photon. Technol. Lett.*, vol. 28, no. 1, pp. 51–54, Jan. 1, 2016.

[12] Z. Yang, W. Xu, and Y. Li, "Fair non-orthogonal multiple access for visible light communication downlinks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 66–69, Feb. 2017.

[13] H. Marshoud, S. Muhaidat, P. C. Sofotasios, S. Hussain, M. A. Imran, and B. S. Sharif, "Optical non-orthogonal multiple access for visible light communication," *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 82–88, Apr. 2018.

[14] M. W. Eltokhey, M. A. Khalighi, and Z. Ghassemlooy, "Dimming-aware interference mitigation for NOMA-based multi-cell VLC networks," IEEE Commun. Lett., doi: 10.1109/LCOMM.2020.3007552.

[15] Q.-V. Pham, T. Huynh-The, M. Alazab, J. Zhao, and W.-J. Hwang, "Sum-rate maximization for UAV-assisted visible light communications using NOMA: Swarm intelligence meets machine learning," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10375–10387, Oct. 2020, doi: 10.1109/JIOT.2020.2988930.

[16] A. Mostafa and L. Lampe, "Physical-layer security for MISO visible light communication channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.

[17] X. Liu, Y. Wang, F. Zhou, S. Ma, R. Q. Hu, and D. W. K. Ng, "Beamforming design for secure MISO visible light communication networks with SLIPT," *IEEE Trans. Commun.*, early access, Aug. 27, 2020, doi: 10.1109/TCOMM.2020.3019818.

[18] T. V. Pham and A. T. Pham, "Energy efficient artificial noise-aided precoding design for visible light communication systems," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Big Island, HI, USA, Feb. 2020, pp. 507–512.

[19] M. A. Arfaoui, A. Ghrayeb, and C. M. Assi, "Secrecy performance of multi-user MISO VLC broadcast channels with confidential messages," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7789–7800, Nov. 2018.

[20] F. Wang, C. Liu, Q. Wang, J. Zhang, R. Zhang, L.-L. Yang, and L. Hanzo, "Optical jamming enhances the secrecy performance of the generalized space-shift-keying-aided visible-light downlink," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 4087–4102, Sep. 2018.

[21] Z. Che, J. Fang, Z. L. Jiang, J. Li, S. Zhao, Y. Zhong, and Z. Chen, "A physical-layer secure coding scheme for indoor visible light communication based on polar codes," *IEEE Photon. J.*, vol. 10, no. 5, pp. 1–13, Oct. 2018.

[22] G. Pan, J. Ye, and Z. Ding, "On secure VLC systems with spatially random terminals," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 492–495, Mar. 2017.

[23] S. Cho, G. Chen, and J. P. Coon, "Physical layer security in multiuser VLC systems with a randomly located eavesdropper," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, Dec. 2019, pp. 1–6.

[24] A. Ijaz, M. M. U. Rahman, and O. A. Dobre, "On safeguarding visible light communication systems against attacks by active adversaries," *IEEE Photon. Technol. Lett.*, vol. 32, no. 1, pp. 11–14, Jan. 1, 2020.

[25] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930–933, May 2016.

[26] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[27] B. M. ElHalawany and K. Wu, "Physical-layer security of NOMA systems under untrusted users," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–6.

[28] K. Cao, B. Wang, H. Ding, T. Li, J. Tian, and F. Gong, "Secure transmission designs for NOMA systems against internal and external eavesdropping," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2930–2943, Mar. 2020.

[29] H. Zhang, N. Yang, K. Long, M. Pan, G. K. Karagiannidis, and V. C. M. Leung, "Secure communications in NOMA system: Subcarrier assignment and power allocation," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1441–1452, Jul. 2018.

[30] H. Lei, J. Zhang, K.-H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.

[31] W. Wu, F. Zhou, R. Q. Hu, and B. Wang, "Energy-efficient resource allocation for secure NOMA-enabled mobile edge computing networks," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 493–505, Jan. 2020.

[32] H.-M. Wang and X. Zhang, "UAV secure downlink NOMA transmissions: A secure users oriented perspective," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5732–5746, Sep. 2020.

[33] Z. Yin, M. Jia, W. Wang, N. Cheng, F. Lyu, and X. Shen, "Max-min secrecy rate for NOMA-based UAV-assisted communications with protected zone," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, Dec. 2019, pp. 1–6.

[34] G. Chopra, R. K. Jha, and S. Jain, "Rank-based secrecy rate improvement using NOMA for ultra dense network," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 10687–10702, Nov. 2019.

[35] X. Zhao, H. Chen, and J. Sun, "On physical-layer security in multiuser visible light communication systems with non-orthogonal multiple access," *IEEE Access*, vol. 6, pp. 34004–34017, 2018.

[36] A. Arafa, E. Panayirci, and H. V. Poor, "Relay-aided secure broadcasting for visible light communications," *IEEE Trans. Commun.*, vol. 67, no. 6, pp. 4227–4239, Jun. 2019.

[37] L. Zhu, Z. Xiao, X.-G. Xia, and D. Oliver Wu, "Millimeter-wave communications with non-orthogonal multiple access for B5G/6G," *IEEE Access*, vol. 7, pp. 116123–116132, 2019.

[38] F. Tariq, M. Khandaker, K.-K. Wong, M. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," Feb. 2019, *arXiv:1902.06700*. [Online]. Available: http://arxiv.org/abs/1902.06700

[39] Cisco, "Cisco visual networking index: Forecast and trends, 2017–2022 white paper," Cisco, San Jose, CA, USA, Tech. Rep., Nov. 2018. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

[40] Y. S. Eroglu, Y. Yapici, and I. Guvenc, "Impact of random receiver orientation on visible light communications channel," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1313–1325, Feb. 2019.
[41] M. D. Soltani, A. A. Purwita, Z. Zeng, H. Haas, and M. Safari, "Modeling the random orientation of mobile devices: Measurement, analysis and LiFi use case," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2157–2172, Mar. 2019.
[42] A. Gupta and P. Garg, "Statistics of SNR for an indoor VLC system and its applications in system performance," *IEEE Commun. Lett.*, vol. 22, no. 9, pp. 1898–1901, Sep. 2018.
[43] F. Miramirkhani, O. Narmanlioglu, M. Uysal, and E. Panayirci, "A mobile channel model for VLC and application to adaptive system design," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1035–1038, May 2017.
[44] P. Chvojka, S. Zvanovec, P. A. Haigh, and Z. Ghassemlooy, "Channel characteristics of visible light communications within dynamic indoor environment," *J. Lightw. Technol.*, vol. 33, no. 9, pp. 1719–1725, May 1, 2015.
[45] S. Ma, Y. He, H. Li, S. Lu, F. Zhang, and S. Li, "Optimal power allocation for mobile users in non-orthogonal multiple access visible light communication networks," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2233–2244, Mar. 2019.
[46] R. Zhang, Y. Cui, H. Claussen, H. Haas, and L. Hanzo, "Anticipatory association for indoor visible light communications: Light, follow me!," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2499–2510, Apr. 2018.
[47] R. Jiang, Q. Wang, H. Haas, and Z. Wang, "Joint user association and power allocation for cell-free visible light communication networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 1, pp. 136–148, Jan. 2018.
[48] J. Tang, M. Dabaghchian, K. Zeng, and H. Wen, "Impact of mobility on physical layer security over wireless fading channels," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 7849–7864, Dec. 2018.
[49] L. Zeng, D. O'Brien, H. Minh, G. Faulkner, K. Lee, D. Jung, Y. Oh, and E. Won, "High data rate multiple input multiple output (MIMO) optical wireless communications using white led lighting," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1654–1662, Dec. 2009.
[50] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[51] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[52] Z. Han, D. Niyato, and W. Saad, *Game Theory in Wireless and Communication Networks*. New York, NY, USA: Cambridge Univ. Press, 2011.
[53] X. Tang, P. Ren, and Z. Han, "Distributed power optimization for security-aware multi-channel full-duplex communications: A variational inequality framework," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 4065–4079, Sep. 2017.
[54] C. Develder, M. De Leenheer, B. Dhoedt, M. Pickavet, D. Colle, F. De Turck, and P. Demeester, "Optical networks for grid and cloud computing applications," *Proc. IEEE*, vol. 100, no. 5, pp. 1149–1167, May 2012.

XIANG ZHAO received the B.S. and M.S. degrees from the Guilin University of Electronic Technology, Guilin, China, in 2001 and 2006, respectively, and the Ph.D. degree in communication and information systems from Xidian University, Xi'an, China, in 2017. Since September 2001, she has been working with the Information and Communication Engineering Department, Guilin University of Electronic Technology, where she is currently an Associate Professor. Her research interests include physical-layer security, visible light communications, reconfigurable intelligent surfaces-assisted wireless communications, and edge computing networks.

JINYONG SUN received the B.S. degree from the Gansu University of Technology, Lanzhou, China, in 2000, the M.S. degree from the Lanzhou University of Technology, Lanzhou, China, in 2003, and the Ph.D. degree in computer science and technology from Xidian University, Xi'an, China, in 2017. Since September 2003, he has been working with the Computer Science and Information Security Department, Guilin University of Electronic Technology, where he is currently an Associate Professor. His research interests focus on information security, semantic communication, machine learning, the Internet of Things, and business process management.